ÇAĞDAŞ CAM SANAYİ VE TİCARET AŞ

BİLGİ GÜVENLİĞİ POLİTİKASI

1. AMAÇ VE KAPSAM

Bu politikanın amacı, **Çağdaş Cam Sanayi ve Ticaret AŞ** (Şirket) bilgi varlıklarının **gizliliğini, bütünlüğünü ve erişilebilirliğini** korumak, bilgi güvenliği risklerini yönetmek ve sermaye piyasası mevzuatına (SPK VII-128.10) tam uyum sağlamaktır. Politika; Şirket bünyesindeki tüm bilgi sistemlerini, kurumsal verileri, iş süreçlerini, tüm çalışanları ve dış hizmet sağlayıcıları kapsamaktadır.

2. BİLGİ GÜVENLİĞİ HEDEFLERİ

- Bilgi varlıklarını iç ve dış tehditlere karşı sürekli korumak ve izinsiz erişimleri önlemek.
- Bilgi güvenliği ihlallerini tespit etmek ve bu olaylara karşı hızlı müdahale mekanizmaları kurmak.
- Yasal ve düzenleyici gerekliliklere (özellikle SPK tebliğlerine) tam uyum sağlamak.
- Tüm personelin bilgi güvenliği farkındalığını yıllık eğitimlerle artırmak.
- **Bilgi güvenliği risklerini** yönetim kurulu tarafından onaylanmış kabul edilebilir seviyelerde tutmak.

3. ROLLER VE SORUMLULUKLAR

- **Yönetim Kurulu:** Politikanın onaylanmasından ve bilgi sistemleri kontrollerinin etkinliğinin gözetilmesinden nihai olarak sorumludur.
- **Üst Yönetim:** Politikanın uygulanmasını gözetir, kritik projeleri onaylar ve bilgi güvenliği için yeterli kaynak tahsis eder.
- **Bilgi Güvenliği Sorumlusu (BGS):** Bilgi sistemleri güvenliğine ilişkin kontrollerin takibinden ve üst yönetime raporlanmasından sorumludur. BGS, bilgi sistemleri yönetimine ilişkin operasyonel bir görev üstlenemez ve doğrudan üst yönetime bağlı çalışır.
- **BT Departman Sorumlusu:** Bilgi sistemleri altyapısının (sunucu, ağ, yazılım vb.) işletiminden, bakımından ve teknik sürekliliğinin sağlanmasından sorumludur. BGS tarafından belirlenen güvenlik kriterlerinin teknik olarak uygulanmasını koordine eder.
- **Tüm Personel:** Şirket'in bilgi güvenliği kurallarına uymak ve şüpheli durumları bildirmekle yükümlüdür.

4. TEMEL GÜVENLİK PRENSİPLERİ

- **Risk Yönetimi:** Bilgi varlıklarına yönelik riskler yılda en az bir kez analiz edilir ve risk seviyelerine göre iyileştirici faaliyetler planlanır.
- **Erişim Yönetimi:** Kullanıcılara yalnızca işleri için gerekli olan **"en az yetki"** atanır. Kritik sistemlere ve uzaktan erişimlere yönelik işlemlerde **Çok Faktörlü Kimlik Doğrulama (MFA)** kullanımı zorunludur.

- **Varlık Yönetimi:** Tüm bilgi varlıkları (donanım, yazılım, veri) envanterde kayıt altına alınır ve kritiklik seviyelerine göre sınıflandırılır.
- **Kayıt ve İzlenebilirlik:** Kritik bilgi sistemleri üzerindeki işlemler ve güvenlik olaylarına ilişkin denetim izleri (loglar) en az **5 yıl** boyunca saklanır.
- **İş Sürekliliği ve Yedekleme:** Kritik süreçleri destekleyen sistemlerin yedekleme stratejisi yazılı hale getirilir ve geri dönüş testleri yılda en az bir kez yapılır. Birincil sistemlerin devre dışı kalması durumunda en geç **24 saat** içinde faaliyetlerin sürdürülmesi esastır.

5. DIŞ HİZMET ALIMI VE ÜÇÜNCÜ TARAFLAR

- Kurumsal kaynak planlama, üretim takip ve ofis/iş birliği sistemleri gibi kritik hizmetlerin alımında; hizmet seviyesi (SLA), veri kaybı hedefi (RPO) ve kurtarma süresi (RTO) değerleri sözleşmelerle netleştirilir.
- Dış hizmet sağlayıcıların Şirket'in bilgi güvenliği standartlarına uyması ve gizlilik yükümlülüklerini yerine getirmesi zorunludur.

6. GÖZDEN GEÇİRME VE YÜRÜRLÜK

Bu politika, yılda en az bir kez veya Şirket yapısında önemli bir değişiklik olduğunda gözden geçirilir; Yönetim Kurulu onayıyla güncellenir ve personele duyurulur.

7. YÜRÜRLÜK

Bu politika, Yönetim Kurulu tarafından onaylandığı tarihte yürürlüğe girer.